RADemics

Secure Firmware Updates in IoT Devices using Hash Based Signature Schemes

Ashish Avasthi, Ramesh Kumar Yadav
POORNIMA UNIVERSITY, THE ICFAI UNIVERSITY

Secure Firmware Updates in IoT Devices using Hash Based Signature Schemes

[1]Ashish Avasthi, Professor, Faculty of Computer Engineering, Poornima University, Jaipur, Rajasthan, India. ashish.avasthi@poornima.edu.in

[2]Ramesh Kumar Yadav, Associate professor, Faculty of Science and Technology, The ICFAI University, Raipur, Chhattisgarh. rameshkumatyadav@iuraipur.edu.in

Abstract

The escalating integration of Internet of Things (IoT) devices into critical infrastructures has underscored the significance of secure firmware management, as firmware remains a foundational yet often overlooked vector for persistent cyberattacks. Firmware vulnerabilities—including unauthenticated updates, insecure bootloaders, and inadequate cryptographic protections—expose IoT ecosystems to tampering, malware injection, and rollback attacks. These challenges are further intensified by the constraints of embedded hardware, diverse deployment environments, and the growing threat of quantum-capable adversaries. Traditional digital signature mechanisms such as RSA and ECC are increasingly inadequate due to their computational demands and lack of post-quantum resilience. This chapter provides a comprehensive analysis of the threat landscape associated with IoT firmware, identifying common architectural weaknesses, attack vectors, and lifecycle vulnerabilities. It highlights the critical role of cryptographic authentication in mitigating these risks and presents hash-based signature schemes (HBSS) as a viable, post-quantum-secure alternative for firmware validation. Emphasis was placed on the integration of HBSS into secure update pipelines, with practical design considerations tailored to resource-constrained devices. The chapter also explores environmental threats, including physical extraction and fault injection, and offers a multi-layered defense framework to enhance firmware integrity. By consolidating recent research, real-world attack scenarios, and cryptographic advancements, this work delivers a strategic blueprint for building resilient IoT systems that can withstand current and emerging firmware-level threats.

Keywords: IoT Security, Firmware Integrity, Hash-Based Signature Schemes, Secure Boot, Post-Quantum Cryptography, Embedded Systems.

Introduction

The exponential growth of Internet of Things (IoT) ecosystems has significantly reshaped industries, urban infrastructure, healthcare systems, and personal technology [1]. These interconnected devices rely on embedded firmware to orchestrate hardware interactions, manage boot processes, and enforce security protocols [2]. As a non-volatile software layer residing within device memory, firmware acts as the first point of execution during startup and maintains persistent control over system functionality [3]. Its critical role in establishing a trusted computing baseline places it at the center of the IoT trust model, this privileged position also renders firmware an attractive target for sophisticated cyber threats [4]. A compromised firmware component can evade traditional runtime protections, manipulate core functionalities, or facilitate undetected long-term

persistence within the system. As a result, firmware has emerged as both a strategic asset and a severe liability within the security posture of modern IoT systems [5].

Its importance, firmware security remains one of the least mature aspects of IoT device development [6]. In many deployments, especially those involving legacy or cost-sensitive hardware, firmware was delivered without rigorous authentication checks or tamper-resistance mechanisms [7]. This lack of validation enables attackers to exploit unsecured update channels, inject unauthorized code, or reinstall vulnerable firmware versions. Update mechanisms are frequently designed for operational simplicity rather than resilience, with minimal protections against rollback attacks, code injection, or partial installations [8]. The issue was further compounded by inconsistent implementation of secure bootloaders, improper public key storage, and insufficient audit mechanisms [9]. As a result, attackers are often able to bypass existing defenses by targeting firmware during critical stages of the device lifecycle—such as boot, update, or memory access—leading to potentially irreversible compromise. These weaknesses demand urgent attention, particularly as the global deployment of IoT systems continues to scale across sensitive domains [10].